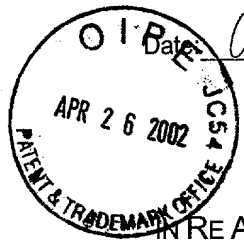I hereby certify that this correspondence is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" Label No. EL 889537452 US in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C., 20231, on:

Date: _April 26, 2002_   By: _Jennifer Mahon_

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF:

Klingler & Tedeschi

SERIAL NO.: 10/028,573

FILED: December 19, 2001

FOR: **SYNCHRONIZATION OF ENCRYPTION IN A WIRELESS COMMUNICATION SYSTEM**

EXAMINER: Not yet Assigned

ART UNIT: 2681

CONFIRMATION NO.:   3290

Preliminary Amendment

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

Prior to examination of the above-identified application, please amend the application as follows:

In the Specification:

Please replace paragraph number [0010] with the following paragraph:

Figure 3A and **Figure 3B** are a block diagram of a message flow for connection establishment for a terminating call in one embodiment.

Please replace paragraph number [0011] with the following paragraph:

Figure 4A and **Figure 4B** are a block diagram of a message flow for connection establishment for and originating call in one embodiment.

Please replace paragraph number [0031] with the following paragraph:

Figures 3A-3B and **4A-4B** illustrate a message flow in one embodiment for connection establishment for a terminating call and an originating call, respectively. A

terminating call is a call in which the RU is the receiver, while the RU is the initiator of an originating call. Referring to **Figures 3A-3B** and **4A-4B**, the respective diagrams each list system layers across the top of the diagram, with base station layers on the left and RU layers on the right. The base station layers and RU layers meet at the physical layer, PHY, as shown. The labeled arrows each represent a message and its direction, that is from base station to RU, or vice versa. The sequence in which the messages occur is illustrated by time advancing from top to bottom in the diagrams.

Repace paragraph number [0032] with the following paragraph:

During the establishment of a telephony connection, before voice data is being transmitted, it is not necessary to encrypt or decrypt data for security. In any case, if encryption mechanisms are not first synchronized between sender and receiver, the voice data may be unintelligible. Therefore, in one embodiment, a place in the message flow is identified that is common to all telephone calls after the DSP initiates a traffic channel, but before any telephony data exchange. As shown in **Figures 3A-3B** and **4A-4B**, both terminating and originating calls use the "set asynchronous balance mode" ("SABM") and "set asynchronous balance mode unnumbered acknowledge" ("SABMUA") messages in their setup. Moreover, the direction of a SABM message is always from RU to base station, while the direction of a SABMUA message is always from base station to RU. In addition, these are LMAC messages that are passed through the ACC processing on the DSP. In one embodiment, it is the ACC processing that encrypts and decrypts the telephony data using the RC4 methodology. Thus, it is convenient to place the mechanism for cryptosystem synchronization at this level of processing. The RC4 methodology is a known encryption/decryption methodology developed by Ron Rivest, and will be explained further below.

Replace paragraph number [0073] with the following paragraph:

Because of the desire to start encryption as close to the start of the traffic channel as possible, (after examining the originating and terminating call setup flows of **Figures 3A-3B** and **4A-4B**) synchronizing each link on the SABM/SABMUA messaging is possible. Uplink is synchronized on SABM, while downlink is synchronized on SABMUA.

Any call setup requires the SABM/SABMUA message transfer. This facilitates the RC4 synchronization maintenance.

In the Drawings:

Please replace Figure 3 with Figures 3A and 3B, enclosed herewith.

Please replace Figure 4 with Figures 4A and 4B, enclosed herewith.

REMARKS

Entry of the above amendments prior to examination is respectfully requested.

Attached hereto is a marked-up version of the changes made to the specification by the current amendment. The attached page(s) is/are captioned **"Version with Markings to Show Changes Made."**

I. <u>Amendments</u>

A. <u>Amendments to the Specification</u>

The specification is amended in accord with the amended figure numbering. Accordingly, no new matter is added by way of these amendments.
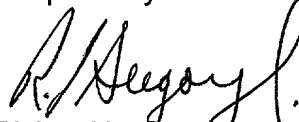
B. <u>Amendments to the Drawings</u>

Figures 3 and 4 are amended in accord with USPTO formal drawing requirements.

No new matter is added by way of these amendments.

If in the opinion of the Examiner a telephone conference would expedite the prosecution of the subject application, the Examiner is encouraged to call Barbara Courtney at (650) 838-4407.

Respectfully submitted,

Date: 4-26-02

Richard L. Gregory, Jr.
Registration No. 42,607

Correspondence Address:
Customer No. 25096
(206) 583-8888

Version with Markings to Show Changes Made

[0010] **Figure 3A** and **Figure 3B** are [is] a block diagram of a message flow for connection establishment for a terminating call in one embodiment.

[0011] **Figure 4A** and **Figure 4B** are [is] a block diagram of a message flow for connection establishment for and originating call in one embodiment.

[0031] **Figures 3A-3B** and **4A-4B** illustrate a message flow in one embodiment for connection establishment for a terminating call and an originating call, respectively. A terminating call is a call in which the RU is the receiver, while the RU is the initiator of an originating call. Referring to **Figures 3A-3B** and **4A-4B**, the respective diagrams each list system layers across the top of the diagram, with base station layers on the left and RU layers on the right. The base station layers and RU layers meet at the physical layer, PHY, as shown. The labeled arrows each represent a message and its direction, that is from base station to RU, or vice versa. The sequence in which the messages occur is illustrated by time advancing from top to bottom in the diagrams.

[0032] During the establishment of a telephony connection, before voice data is being transmitted, it is not necessary to encrypt or decrypt data for security. In any case, if encryption mechanisms are not first synchronized between sender and receiver, the voice data may be unintelligible. Therefore, in one embodiment, a place in the message flow is identified that is common to all telephone calls after the DSP initiates a traffic channel, but before any telephony data exchange. As shown in **Figures 3A-3B** and **4A-4B**, both terminating and originating calls use the "set asynchronous balance mode" ("SABM") and "set asynchronous balance mode unnumbered acknowledge" ("SABMUA") messages in their setup. Moreover, the direction of a SABM message is always from RU to base station, while the direction of a SABMUA message is always from base station to RU. In addition, these are LMAC messages that are passed through the ACC processing on the DSP. In one embodiment, it is the ACC processing that encrypts and decrypts the telephony data using the RC4 methodology. Thus, it is convenient to place the mechanism for cryptosystem synchronization at this level of processing. The RC4 methodology is a

known encryption/decryption methodology developed by Ron Rivest, and will be explained further below.

[0073] Because of the desire to start encryption as close to the start of the traffic channel as possible, (after examining the originating and terminating call setup flows of **Figures 3A-3B** and **4A-4B**) synchronizing each link on the SABM/SABMUA messaging is possible. Uplink is synchronized on SABM, while downlink is synchronized on SABMUA. Any call setup requires the SABM/SABMUA message transfer. This facilitates the RC4 synchronization maintenance.